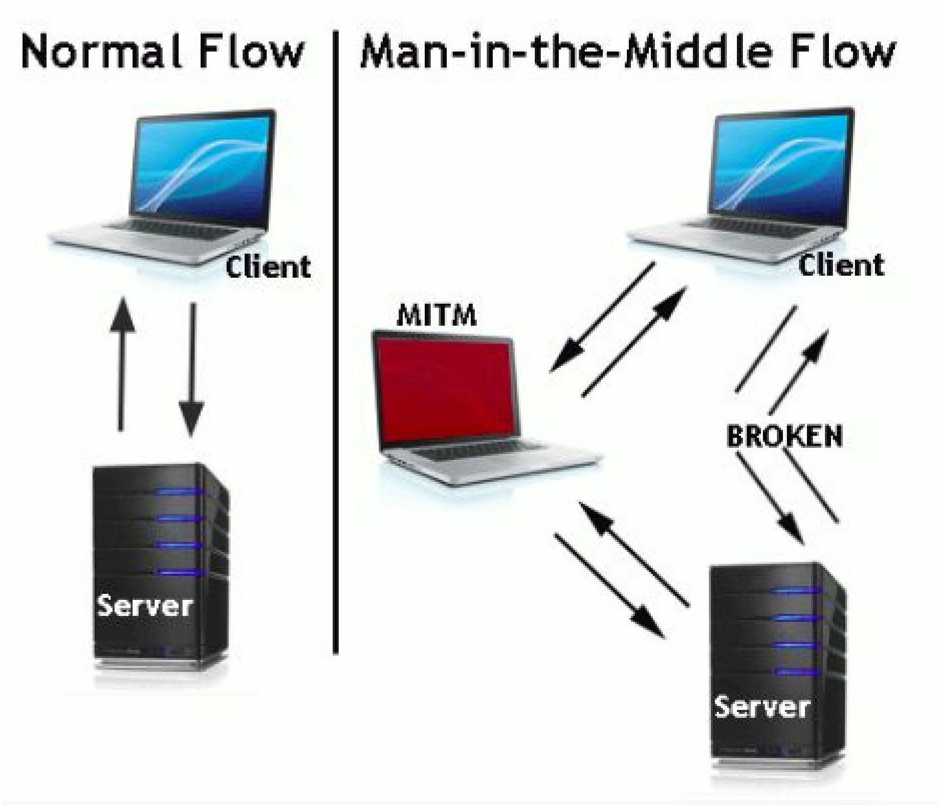
MAN IN THE MIDDLE (MITM) ATTACK

A man-in-the-middle attack is a type of cyberattack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM.

Key Concepts of a Man-in-the-Middle Attack

- Man-in-the-middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems.
- A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.
- Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.

Man-in-the-Middle Attack Examples



Types of Man-in-the-Middle Attacks

Rogue Access Point

Devices equipped with wireless cards will often try to auto connect to the access point that is emitting the strongest signal. Attackers can set up their own wireless access point and trick nearby devices to join its domain. All of the victim's network traffic can now be manipulated by the attacker. This is dangerous because the attacker does not even have to be on a trusted network to do this—the attacker simply needs a close enough physical proximity.

ARP Spoofing

ARP is the Address Resolution Protocol. It is used to resolve IP addresses to physical MAC (media access control) addresses in a local area network. When a host needs to talk to a host with a given IP address, it references the ARP cache to resolve the IP address to a MAC address. If the address is not known, a request is made asking for the MAC address of the device with the IP address.

An attacker wishing to pose as another host could respond to requests it should not be responding to with its own MAC address. With some precisely placed packets, an attacker can sniff the private traffic between two hosts. Valuable information can be extracted from the traffic, such as exchange of session tokens, yielding full access to application accounts that the attacker should not be able to access.

mDNS Spoofing

Multicast DNS is similar to DNS, but it's done on a local area network (LAN) using broadcast like ARP. This makes it a perfect target for spoofing attacks. The local name resolution system is supposed to make the configuration of network devices extremely simple. Users don't have to know exactly which addresses their devices should be communicating with; they let the system resolve it for them. Devices such as TVs, printers, and entertainment systems make use of this protocol since they are typically on trusted networks. When an app needs to know the address of a certain device, such as tv.local, an attacker can easily respond to that request with fake data, instructing it to resolve to an address it has control over. Since devices keep a local cache of addresses, the victim will now see the attacker's device as trusted for a duration of time.

DNS Spoofing

Similar to the way ARP resolves IP addresses to MAC addresses on a LAN, DNS resolves domain names to IP addresses. When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name, such as www.onlinebanking.com. This leads to the victim sending sensitive information to a malicious host, with the belief they are sending information to a trusted source. An attacker who has already spoofed an IP address could have a much easier time spoofing DNS simply by resolving the address of a DNS server to the attacker's address.

Man-in-the-Middle Attack Techniques

Sniffing

Attackers use packet capture tools to inspect packets at a low level. Using specific wireless devices that are allowed to be put into monitoring or promiscuous mode can allow an attacker to see packets that are not intended for it to see, such as packets addressed to other hosts.

Packet Injection

An attacker can also leverage their device's monitoring mode to inject malicious packets into data communication streams. The packets can blend in with valid data communication streams, appearing to be part of the communication, but malicious in nature. Packet injection usually involves first sniffing to determine how and when to craft and send packets.

Session Hijacking

Most web applications use a login mechanism that generates a temporary session token to use for future requests to avoid requiring the user to type a password at every page. An attacker can sniff sensitive traffic to identify the session token for a user and use it to make requests as the user. The attacker does not need to spoof once he has a session token.

SSL Stripping

Since using HTTPS is a common safeguard against ARP or DNS spoofing, attackers use SSL stripping to intercept packets and alter their HTTPS-based address requests to go to their HTTP equivalent endpoint, forcing the host to make requests to the server unencrypted. Sensitive information can be leaked in plain text.

Preventing Man-in-the-Middle Attacks

Strong WEP/WAP Encryption on Access Points

Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force his way into a network and begin man-in-the-middle attacking. The stronger the encryption implementation, the safer.

Virtual Private Network

VPNs can be used to create a secure environment for sensitive information within a local area network. They use key-based encryption to create a subnet for secure communication. This way, even if an attacker happens to get on a network that is shared, he will not be able to decipher the traffic in the VPN.

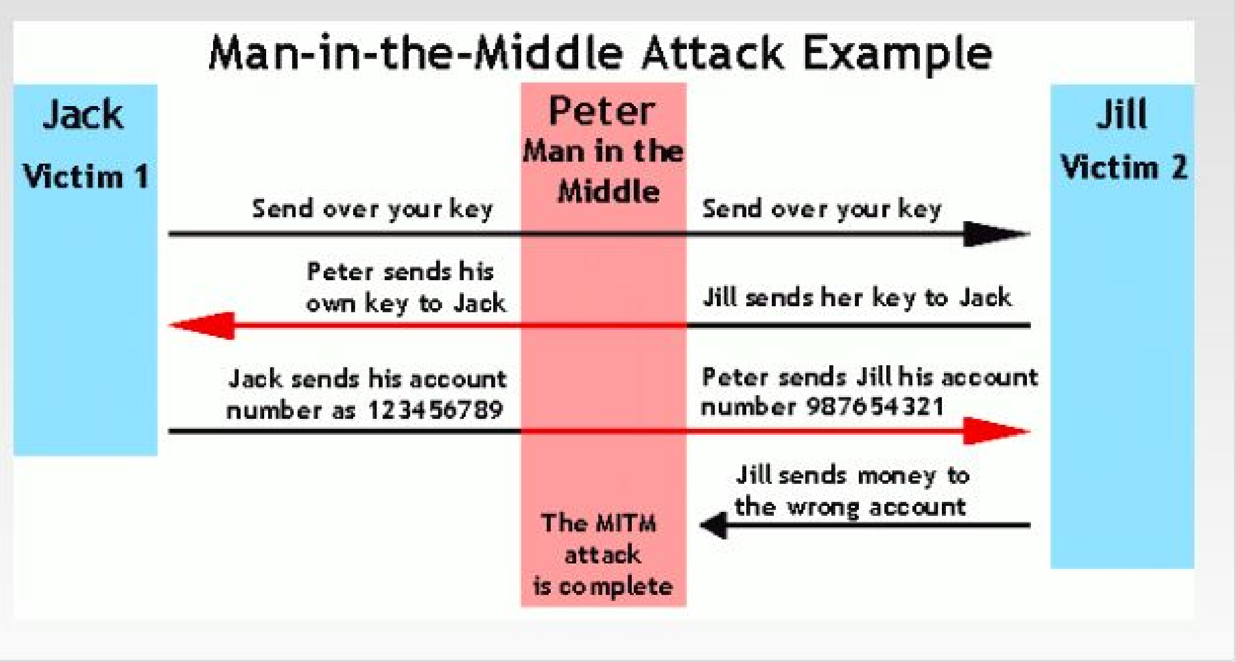
Force HTTPS

HTTPS can be used to securely communicate over HTTP using public-private key exchange. This prevents an attacker from having any use of the data he may be sniffing. Websites should only use HTTPS and not provide HTTP alternatives. Users can install browser plugins to enforce always using HTTPS on requests.

Public Key Pair Based Authentication

Man-in-the-middle attacks typically involve spoofing something or another. Public key pair based authentication like RSA can be used in various layers of the stack to help ensure whether the things you are communicating with are actually the things you want to be communicating with.

Below is an **example** of what might happen once the man in the middle has inserted him/herself.


Man-in-the-Middle Attack Example
Jack
Victim 1
Peter
Man in the Middle
Jill
Victim 2
Send over your key
Send over your key
Peter sends his own key to Jack
Jill sends her key to Jack
Jack sends his account number as 123456789
Peter sends Jill his account number 987654321
Jill sends money to the wrong account
The MITM attack is complete

The hacker is impersonating both sides of the conversation to gain access to funds. This example holds true for a conversation with a client and server as well as person-to-person conversations. In the example above, the attacker intercepts a public key and with that can transpose his own credentials to trick the people on either end into believing they are talking to one another securely.